

REMARKS

Claims 1-12 and 14-24 were pending in the application. Claim 1 has been amended to require that the document visually setting forth obligations to which the user is to be contractually bound upon assent to the obligations by the user. Claims 4, 5, 7 and 8 are also amended to include language more technically correct and to clarify the scope of the claims. New claim 25 is similar to previous pending claim 1, but now requires that the document is one that is to be viewed and signed so that the document cannot be repudiated. Additionally, claim 25 incorporates the limitations of claim 6. Claims 7 and 22 have been amended to depend from new claim 25. Support for the amendments of claim 1 and 25 are found, for example, on page 13, paragraph 2 and page 14, paragraph 3 of the specification. No new subject matter is believed to have been added by these amendments. Therefore, claims 1-12 and 14-25 remain in this application.

Objections to the Specification

Applicant has cancelled the previously added material to the Abstract viewed as new matter by the Examiner. Accordingly, Applicant respectfully requests that the Examiner withdraw the new matter rejection.

35 U.S.C. § 112 Rejections

Claims 4 and 5 and the intervening claims stand rejected under 35 U.S.C. § 112, first paragraph, for failing to comply with the written description requirement. Specifically, the Examiner notes that claims 4 and 5 refer to various events not occurring until the audit means audits the signing/validation, and asserts that Applicant's disclosure does not "convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention."

Applicant believes the confusion has probably occurred through a rather specialized use of the verb "audits" in the sense of "to add to the audit log." This is in

contrast to the more common use of “reviewing material in the audit log.” Applicant has changed occurrences of this verb in claims 4, 5, and 20 to the phrase “records in an audit trail a record of.” The recording of such information into audit trails for retrospective security is well known to those of ordinary skill in the art. It is described in, for example, http://www.windowsecurity.com/whitepaper/NCSCTG001_Tan_book.html and http://en.wikipedia.org/wiki/Audit_trail. Accordingly, Applicant respectfully requests that the Examiner withdraw the indefiniteness rejection.

35 U.S.C. § 103 Rejections

Claims 1, 4, 5, 10, 14 and 17-24 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 5,917,913 to Wang in view of U.S. Patent No. 6,092,202 to Veil et al. (hereinafter “Veil”). Specifically, the Examiner continues to assert that prior art discloses display of a “document,” and cites examples from Wang: “purchase transaction, bank transaction, library materials transaction, financial transactions, vendor/user transaction etc.” Accordingly, the Examiner asserts that this disclosure meets the recitation of “data including a [the] document” of instant claim 1.

Furthermore, claims 2, 3, 9 and 15-16 stand rejected under 35 U.S.C. § 103(a) as being obvious over Wang in view of Veil as applied to claim 1, and further in view of Bruce Schneier, Applied Cryptography, 1996, John Wiley & Sons, Second Edition, pp. 43-44 (hereinafter “Schneier”). Additionally, claims 11-13 stand rejected under 35 U.S.C. § 103(a) as being obvious over Wang in view of Veil as applied to claim 1, and further in view of U.S. Patent No. 5,742,756 to Dillaway et al. (hereinafter “Dillaway”). Also, claims 6-8 stand rejected under 35 U.S.C. § 103(a) as being obvious over Wang in view of Veil as applied to claim 1, and further in view of U.S. Patent No. 6,408,388 to Fisher (hereinafter “Fisher”).

In response to the Examiner’s continued §103(a) rejections, Applicant asserts that:

- (a) a “transaction” is not the same as a “document”, but rather a transaction is only a very specific and limited type of document;
- (b) while Wang has disclosed display of a transaction, he has not disclosed the display of a general document;
- (c) the Applicant’s specification refers to documents in general as distinct from specific and limited subclass of documents;
- (d) it is non-obvious to one of ordinary skill in the art to extend Wang’s display of transactions to the display of documents;
- (e) Wang discloses the signing of a transaction, but has not disclosed that he has considered the possibility that the transaction may be different from the one he is expecting; and
- (f) it is non-obvious for one of ordinary skill in the art to make the connection to extend Wang’s PEAD with Veil’s trusted display.

The following sections provide evidence and discussion in support of Applicant’s assertions.

(a) On the difference between Documents and Transactions

Applicant used two approaches to assess the relationship between these words: firstly, the Merriam-Webster dictionary (accessed online at <http://www.m-w.com>), and secondly the Google search for definitions.

1. Merriam-Webster Dictionary

Applicant chose to use this Dictionary as representative of general usage of words in the USA. The entries for “document” and “transaction” are as follows:

Main Entry: ¹**doc·u·ment**

Pronunciation: ‘dä-ky&-m&nt

Function: noun

Etymology: Middle English, from Middle French, from Late Latin & Latin; Late Latin documentum official paper, from Latin, lesson, proof, from docEre to teach -- more at DOCILE

1 a archaic : PROOF, EVIDENCE b : an original or official paper relied on as the basis, proof, or support of something c : something (as a photograph or a recording) that serves as evidence or proof

2 a : a writing conveying information b : a material substance (as a coin or stone) having on it a representation of thoughts by means of some conventional mark or symbol c :

DOCUMENTARY

- doc·u·men·tal /ˈdä-ky&-ˈmen-t&l/ adjective

Main Entry: **trans·ac·tion**

Pronunciation: tran-ˈzak-sh&n, tran(t)-ˈsak-

Function: noun

1 a : something transacted; especially : an exchange or transfer of goods, services, or funds <electronic transactions> b plural : the often published record of the meeting of a society or association

2 a : an act, process, or instance of trans acting b : a communicative action or activity involving two parties or things that reciprocally affect or influence each other

- trans·ac·tion·al /-shn&l, -sh&-n&l/ adjective

It is reasonable to ignore archaic usage. Applicant sees therefore that “document” has a very broad meaning (2a): “a writing conveying information.” Meaning 2b refers to the physical medium on which the writing is made. When Applicant considers documents on computers, this meaning is less relevant.

For “transaction,” the particular definition exemplified by “electronic transactions” (which makes it especially appropriate for the purposes of assessing these patents) is “an exchange or transfer of goods, services, or funds.”

Definition 1b is a specific use of the term transaction distinct from this sense. Although “a published record of a meeting” seems to broaden the meaning of the term, it does not do so to the extent required to make document and transaction synonymous. Applicant further notes that there is no indication that Wang or Veil has made use of the term in this sense.

The 2a definition of transaction is more general and more abstract, and thus it encompasses a wider variety of entities than, but also including, the first definition. Again, there is nothing in Wang or Veil that indicates use of the term in any sense that is not included in the examples given in definition of 1a.

2. Google definitions search

Google can provide a list of definitions of a word that it has found on the Internet. It ranks these according to its measure of the authority and popularity of the citation. Applicant learned more about the practical applications of terms by examining definitions as used by a variety of specialist domains with this method.

Google reports the following definitions of document (located by entering “define:document” in the Google search page:

<http://www.google.com.au/search?num=100&hl=en&q=define%3Adocument>).

Definitions of **document** on the Web:

1. Writing that provides information (especially information of an official nature)
2. Anything serving as a representation of a person’s thinking by means of symbolic marks
3. A written account of ownership or obligation
4. Record in detail; “The parents documented every step of their child’s development”
5. Text file: (computer science) a computer file that contains text (and possibly formatting instructions) using seven-bit ASCII characters
6. Support or supply with references; “Can you document your claims?”
wordnet.princeton.edu/perl/webwn
7. A document is a writing that contains information.
en.wikipedia.org/wiki/Document
8. Document is an album by R.E.M.. It was released in 1987 and is the last album of new material by the band released under the I.R.S. Records label. The words “File Under Fire” appear on the cover and many of the songs include references to fire.
[en.wikipedia.org/wiki/Document_\(album\)](http://en.wikipedia.org/wiki/Document_(album))
9. A file created using an application. For example, you might create a text document using a word processing application (such as Word) or a picture document using a graphic application (such as Paint Shop Pro).
www.visionsofadonai.com/onrampglossary.html
10. Generic term for any piece of paper with important data such as an invoice, inventory sheet, application, etc.

www.theaccountspayablenetwork.com/html/modules.php

11. Unit of information sent from servers to clients; a document may contain plain or formatted text, in-lined graphics, sound, other multi-media data, or hyperlinks to other documents; often also referred to as a file
www.muelec.fpms.ac.be/home/mosaic/MBook_53.html
12. When used in reference to the World Wide Web, a document is any file containing text, media or hyperlinks that can be transferred from an HTTP server to a client program.
www-personal.umich.edu/~zoe/Glossary.html
13. An item of information that users want to retrieve. It could be a text file, a Web page, a newsgroup posting, a picture, etc.
cavalierwebsolutions.com/seoglossary.html
14. Any item (not necessarily on paper) that can be indexed or catalogued.
members.optusnet.com.au/~webindexing/Webbook2Ed/glossary.htm
15. Digital object that is the analog of a physical document, especially textual materials; a document model is an object model for documents.
www.cs.cornell.edu/wya/DigLib/MS1999/glossary.html
16. 1. Noun: a paper which establishes certain facts or attempts to bring about a certain result. 2. Verb: to set out events, facts or beliefs in written form.
www.search4miamihomes.com/realestateglossary/D.html
17. HTML document.
www.cs.indiana.edu/elisp/w3/docs/w3_17.html
18. As used in EDI, one complete piece of data. For example, one Purchase Order, or one Invoice. Also known as a "Message"
www.bcbsks.com/providers/edi/glossary.htm
19. For the purposes of this standard, an HTML instance.
www.w3.org/MarkUp/html3/terms.html
20. A "textual object." In HTML, documents (or "pages") were single files containing HTML. In XML, documents may contain content from several files or chunks and should included mark-up structures that make it valid or well-formed.
www.daisy.org/publications/guidelines/sg-daisy3/glossary.htm
21. 1. The physical entity of any printed work, such as a book or manuscript; material on which information has been recorded; 2. a government publication or public document.
www.fsu.edu/library/search/glossary.shtml

22. The physical entity which contains recorded information--books, graphics, audio recordings, etc. may be called documents. Documentation
www.sir.arizona.edu/resources/glossary.html
23. Recorded information that is made or received in the course of a practical activity.
www.library.utoronto.ca/utarms/info/glossary.html
24. A book, article, pamphlet, etc. A government document is a book, pamphlet, or other item that has been published by the State or United States Government.
www.wcu.edu/library/researchref/Glossary.htm
25. An original or official paper or publication.
library.albany.edu/usered/basics/libterm.html
26. A document is a set of information designed and presented as an individual entity. A publication is a good example of a document. It may contain logical subunits such as parts, sections, or chapters; but it is typically created, updated, and presented as a single unit. The World Wide Web (WWW) presentation of a document may consist of one or many WWW pages.
www.umich.edu/Textonly/policy_guidelines6.html
27. This refers to the entire body of information comprising this project. In particular, the document may be categorized by naming the nodes in it, specifying the context of the individual nodes, and describing the links connecting nodes.
ai.eecs.umich.edu/cogarch0/reader/definitions.html
28. Means any written, printed, recorded, magnetic, graphic matter, or other documentary material, regardless of form or characteristic.
www.nrc.gov/reading-rm/doc-collections/cfr/part002/part002-1001.html
29. A programming object containing information that originates with the user of the application, rather than created by the application itself. The data for documents usually is stored in disk files.
docs.rinet.ru/NTServak/glossary.htm
30. A Drawing or a Block .
www.ribbonsoft.com/qcad_doc_glossary.html
31. A file that a user can create and edit. A document is usually associated with a single application, which the user expects to be able to open by double-clicking the document's icon in the Finder.
developer.apple.com/documentation/mac/Files/Files-389.html
32. The unit of documentation management in GSyC-doc. For instance it can be a paper, a book, a FAQ, or whatever its author considers a having enough entity to become an independent document. Documents can be compiled and installed in isolation of other documents. Usually, each directory will contain just one document, and each

document will be contained in just one directory.
gsyc.escet.urjc.es/gsync-doc/node1.html

33. 1. The combination of a medium and the information recorded on or in it which may be used as evidence or for consultation 2. A single record or item. Examples include: a sheet of paper with writing; an E-Mail message; a film with images; a magnetic tape with a sound recording.
www.unesco.org/webworld/mdm/administ/en/guide/guide011.htm

Google reports the following definitions for transaction:

Definitions of **transaction** on the Web:

1. The act of transacting within or between groups (as carrying on commercial activities); "no transactions are possible without him"; "he has always been honest in his dealings with me"
wordnet.princeton.edu/perl/webwn
2. Means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:
<https://www.rascal.columbia.edu/comply/hipaaglossary.html>
3. The process that takes place when a cardholder makes a purchase with a credit card.
www.vpsource.com/glossary.html
4. The entry or liquidation of a trade.
www.cftc.gov/opa/glossary/opaglossary_t.htm
5. An inseparable list of database operations which must be executed either in its entirety or not at all. Transactions maintain data integrity and guarantee that the database will always be in a consistent state. Transactions should either end with a COMMIT or ROLLBACK statement. If it ends with a COMMIT statement, all the changes made to the database are made permanent. If the transaction fails, or ends with a ROLLBACK, none of the statements takes effect. Also see LUW.
www.orafaq.com/glossary/faqglost.htm
6. The buying or selling of currencies resulting from the execution of an order.
www.fx-forex-trading.com/glossary.htm
7. may include application fees; title examination, abstract of title, title insurance, and property survey fees; fees for preparing deeds, mortgages, and settlement documents; attorneys' fees; recording fees; and notary, appraisal, and credit report fees. Under the Real Estate Settlement Procedures Act, the borrower receives a good faith estimate of closing costs at the time of application or within three days of application. ...
www.reallifedebt.com/mortgage-and-loan-terminology-glossary.shtml

8. Action between a cardholder and a merchant or a cardholder and a member that results in activity on the cardholder account.
www.1stamericancardservice.com/Glossary.html
9. An order to buy or sell securities that has been executed.
www.firstrepublicbrokerage.com/republic/invest_glosry_TnTz.htm
10. The basic focus of reader-response criticism on the negotiation or collaboration between author, text, and reader that determines literary meaning. (See also discourse.)
www2.cumberlandcollege.edu/acad/english/litcritweb/glossary.htm
11. An "an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs." UETA 2(16).
euro.ecom.cmu.edu/resources/elibrary/eclgloss.shtml
12. A group of related database changes that are written to the database as a single unit during a commit. The logical consistency of a database is maintained by placing all related updates within transactions.
www.ittia.com/dbstar/manual/UG_Gloss.htm
13. (1) Any agreement between two or more parties that establishes a legal obligation. (2) The act of carrying out such an obligation. (3) All activities affecting a deposit account that are performed at the request of the account holder. (4) All events that cause some change in the assets, liabilities or net worth of a business. (5) An action between a cardholder and a merchant or a cardholder and a member that results in activity on the cardholder account.
www.creditcards.com/credit-cards-glossary.php
14. The smallest unit of business activity. Uses of records are themselves transactions.
www.records.curtin.edu.au/recordkeeping_manual/glossary.html
15. An agreement between a buyer and a seller to exchange an asset for payment. Or in accounting, any event or condition recorded in the books of account.
www.unisys.com/common/investors/glossary/t.asp
16. Any agreement between a vendor and a consumer for provision of a good or service.
cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00065e.html
17. Term used whenever an action is taken against an outstanding order (bid or ask). Possible actions are a consummated sale, an expiration of an order, and cancellation of an order due to its infeasibility.
www.biz.uiowa.edu/iem/trmanual/IEMManual_4.html
18. To carry through or bring about.
library.thinkquest.org/J003358F/terms.html
19. Any dealing or action that involves crossing a boundary from one status or participant to another. Transactions of sufficient importance may require a record attesting to

what has occurred
john.curtin.edu.au/society/glossary/

20. Services provide facilities for grouping operations into atomic units, called transactions, with the certainty that a transaction will be carried out in its entirety or not at all. This corresponds to some of the transaction manager services in the Transaction Processing service category.
www.opengroup.org/architecture/togaf7-doc/arch/p3/trm/tx/tx_objec.htm
21. 1. Individual event (such as receipts, issues, and transfers) reported to the computer system. 2. A group of one or more message fields. 3. A transaction is made up of a header and a group of fields. For example, a work order transaction might have a transaction type and three fields consisting of a work order number, part number, and due date.
www.intermec.com/eprise/main/Intermec/Content/About/GlossarySubpages/Glossary_ST
22. The proceedings of a society, convention, etc., especially a published one.
www.seattlecentral.org/faculty/jshoop/glossary.html
23. An ACH transaction is an entry within the NACHA file that indicates how the participant's account should be affected. The transaction includes a reference to the participant, how the account is affected, and the amount.
www.exchangebank.com/business/cash_management/glossary.asp
24. A single activity within a computer system, such as an entry into an airline reservation database, that is executed in real time rather than as a batch process. (Ref: Dyson, Dictionary of Networking)
www.labcompliance.com/glossary/r-t-glossary.htm
25. A collection of related messages designed to complete (insofar as this is possible) the intention of the initiator of the original message, and normally concluded by a debit or credit transaction. Amendments or reversals carried out subsequently are to be considered as a separate transaction set.
www.transcan.com/glossary.html
26. A mechanism to group a series of service invocations into a single operation. Transactions are used to make sure that either the entire series of service invocations take effect, or that none of them do. An LNS host application can explicitly manage transactions or it can let the NSS implicitly start and commit transactions as needed.
www.echelon.com/support/KnowledgeDB/FAQ_Glossary/glossary4.htm

Of note, when comparing these definitions, "document" is a much more general term than "transaction."

By using Google to locate definitions, Applicant obtains a set that is biased towards usage in Information Technology and related fields. However, this is reasonable,

because that covers the domain being considered by Wang, Veil, Fischer, Dillaway and the present application. In this field, Applicant finds that “document” may refer to information that is stored in a computer file (see definitions 5, 9, 11, 12, 13, 17 and others).

In some specific fields, such as electronic data interchange for health services, “document” can be very closely related to a “transaction” (see definition 18). However, the breadth of definitions provided, and the specificity of that application means that Applicant cannot reasonably conclude that “document” and “transaction” are synonymous in the current patent examination.

We also note that “transaction” has a specific technical meaning in relation to databases (see definitions 5, 12, 20, 21, 24, 25, 26) which appears to be different from the meaning considered by Wang and Veil. It might be suggested that extending the approval process from a financial (or related) transaction to a database transaction would be obvious to one of ordinary skill in the art. However, even this would be debatable. Whereas the exchange of currency or other goods or services of value (the most common definition of transaction) is clearly something to which security is applicable, it is not at all clear that there would be a benefit to obtaining specific user approval for generic database transactions. Applicant asserts that it is not obvious to extend transaction from its common meaning to another database-specific meaning of the same word, let alone to the meaning of document.

(b) Wang’s Disclosure and Veil’s Disclosure refer to Transactions

Wang’s abstract refers to a “device for approving a transaction”.

Wang’s background opens with the statement “The present invention relates to methods and apparatus for conducting electronic transactions.”

We can see that the examples given by Wang (column 1, lines 16-32) of electronic transactions clearly fit and span the meaning of “transaction”, but not “document”.

His examples are:

- Automatic teller machines (withdrawals, transfers, deposits);
- Automated point of sale systems;
- Automated library systems (check out and return library materials); and
- Making a purchase from a vendor on the network.

Veil, column 4, lines 28-30: *A majority of the application programs for conducting electronic transactions (electronic transactions applications) are executable on one of the conventional operating system platforms such as OS/2, Windows, Unix, etc.*

From this, it seems that Veil is talking about *existing* applications that are reasonably common.

Veil, column 7, line 58 - column 8 line 2: *The trusted display is separate and can be significantly different from the display of the computer. The trusted display is a dedicated display used for displaying data representing true transaction information such as transaction amount(s). The trusted display can be, for example, a small LCD display or alike. When the security coprocessor processes transactions, it also gains access to the true transaction value(s) or amount(s). Therefore the security coprocessor can provide the true transaction amount(s) to the trusted display, and guarantee that the amount(s) displayed correctly represent the values of the electronic transactions in progress.*

From this, it seems that Veil expects that a transaction is limited to a financial transaction - one that has a “value” or an “amount.”

Veil, column 8 lines 3-8: *The computer user can compare the transaction amount(s) displayed on the trusted display with amount(s) displayed on the display of the computer. For example, in an electronic transaction involving exchange of goods or transfer of money, a \$5000 transaction may be shown as only a \$500 transaction on the computer display.*

This is further evidence that Veil only considers transactions of a financial nature.

(c) Applicant's Application refers to (general) Documents

Page 1 mentions "economic value of information and transactions being handled digitally".

The title and background of this application refers to digital signatures.

On page 4, the Digital Signature Semantics section talks about "signing a document," and says "Documents requiring signatures include, but are not restricted to, personal letters, contracts, or cheques."

On page 5, Applicant talks about a "digitally signed message or document."

On page 9, "Endpoint Attack," Applicant says "sign an email message." Note that the UNESCO definition of document explicitly includes an Email message as an example.

On page 12, Applicant gives further examples of data sent to the Digital Private Key Protection Device (hereinafter "DPKPD") for signature: "a shopping order list, a military command to fire a missile, or a contract."

One page 13, Applicant says "Once the user has read and understands the document displayed..." and "If the user agrees with or authorises the contents of the document, just as they would in the paper domain, they can choose to digitally sign the document."

This strongly suggests that any paper document that might be signed is a candidate for signing in the electronic world. This clearly is more than just "transactions."

On page 23, Applicant notes that a DPKPD could be used to create (public key) Certificates, and describe how the double-signing aspects previously used for general "documents" would be useful for public key certificates. This demonstrates Applicant's

intent that the DPKPD should be able to sign a wide variety of types of information – documents in the most general sense – rather than specific transactions.

Also on page 23, the last paragraph opens with “Figure 3 depicts a message text (document) which has....” Again, this supports the view that any message can be signed.

As a further example of the applications of a DPKPD, Applicant describes on page 29 how it could be used to authorize “transactions.”

(d) Not obvious to extend display of transactions to display of documents

There are many systems in the world today that facilitate the electronic approval of transactions. Two very common examples are:

EFTPOS terminals typically display the amount of a transaction on the screen while asking a user to select an account, and enter a PIN or press OK.

Internet Banking systems typically allow a user to specify details of a transaction, and then display those details again and ask for confirmation, before actioning the transaction.

In contrast, there are very few mechanisms that will display a general document to the user before a digital signature is applied. For example, email programs such as Microsoft Outlook or Netscape Communicator simply allow the user to select an option to sign messages, without specifically re-displaying the message for approval.

A recent development (after the date of Applicant’s patent application) is that the Australian Tax Office and other Australian government departments that deal electronically with businesses have developed the “Common Signing Interface” (<http://csi.business.gov.au/CSI/Welcome.asp>) for applying digital signatures. In this case, the user’s software displays the document (which may be a transaction) to the user for the user to peruse before he or she agrees to apply a digital signature (with the legal consequences that

that implies). Applicant notes that this mechanism is still vulnerable to the Endpoint Attack described in the application.

One key difference which distinguishes the ability to review transactions from the ability to review documents is that the amount of information that needs to be displayed. Wang's example (Fig 6A) shows a small device with a screen that displays a single line of approximately 9 characters at a time ("TR # 4096"). EFTPOS terminals also typically only show 1-4 lines of text that invite a consumer to choose an account (Check, Savings, or Credit), to approve the amount of the transaction, and to enter a PIN. It is very simple to develop a portable or handheld device that can display this information. People of ordinary skill in the art would not find it obvious to adapt this technology to the display of "documents" (such as contracts) which may consist of tens of pages. None of the prior art patents teach or provide motivation to adapt their inventions to deal with documents.

Veil's invention refers specifically to smart cards. To determine whether it might be obvious for one of ordinary skill in the art to extend from approving transactions to approving documents, Applicant assessed the areas in which smart cards are ordinarily used. Two authoritative sources that could reasonably describe common uses for smart cards are Wikipedia and How Stuff Works.

Wikipedia (http://en.wikipedia.org/wiki/Smart_card) nominates:

- Credit or ATM cards
- SIMs for mobile phones
- Authorisation cards for pay television
- High security identification and access control cards
- Public transport payment cards
- Electronic wallets
- Digital identification (authentication of identity)

How Stuff Works (<http://electronics.howstuffworks.com/question332.htm>) nominates:

- Credit cards
- Electronic cash
- Computer security systems

- Wireless communication
- Loyalty systems (like frequent flyer points)
- Banking
- Satellite TV
- Government identification
- Mobile phones
- Vending machines

While it may be tempting to claim that the DPKPD is a computer security application, the type of computer security application that How Stuff Works refers to is authentication of a user – not letting a person log on unless they have the correct smart card (as well as the correct password and/or biometric).

These applications can be divided into three categories:

- transaction systems (credit and ATM cards, public transport payment, electronic wallets, electronic cash, banking, loyalty, vending machines),
- portable PIN-protected id systems (mobile phones, access control card, government identification, computer security) and
- portable containers for a decryption key (pay television, satellite TV, wireless communication).

The DPKPD application of signing or approving general documents (apart from transactions) is not part of any of these three fields. It cannot be argued that approving documents is an obvious application of the concept of Wang and Veil to other areas where smart cards are used.

(e) Wang's signing of files

Wang does teach (column 12, line 65 – column 13 line 2) that his PEAD could be used to apply signatures to files “for authentication purposes (e.g. to authenticate the date or the user).”

Wang has one “method” claim (72) that starts “The method of claim 63 further comprising displaying said transaction request for viewing by said user on a display screen.”

Claim (82) is the only one that refers to signing files: “The method of claim 63 wherein said transaction request represents a request for authenticating an electronic file....”

Some important aspects of this are:

(a) Wang does not mention displaying the file.

(b) Wang does not mention that there would be an opportunity for the user to review the contents of the file before signing it.

(c) “To authenticate the date or user” strongly suggests that Wang is aware of the threat that one user may impersonate another by using private key details on a computer, and Wang counters this threat by using the PEAD instead of a private key on the computer. However, Wang’s application shows no evidence that he has considered the possibility that the file (or indeed a transaction) may be different from the one he is expecting, and therefore there is no reason to suspect that Wang would want (or see a need) to review the contents of the file. There is certainly nothing in the patent that teaches “display of the document.”

(d) There is nothing to suggest that Wang’s display of a transaction request includes *all* details of the transaction.

(e) There is nothing to suggest that Wang contemplated the operation of claims 82 and 72 together.

(f) Even if claims 72 and 82 were embodied together, and even if the whole transaction request were displayed, there is nothing to suggest that the portion of the file that is to be signed would be displayed.

(f) Wang in light of Veil

The Examiner has cited column 10, line 65 - column 11, line 12 of Wang as evidence that Wang has taught the use of a display. The Examiner says (paragraph 5.2) that it would be obvious to one of ordinary skill in the art to modify this display to guarantee that it represented the true transaction information as suggested by Veil.

(f1) Not Obvious to combine Wang and Veil

Applicants do not agree that it would have been obvious for one of ordinary skill in the art to make the connection to extend Wang's PEAD with Veil's trusted display.

Many security inventions by people of ordinary skill in the art rely on "regular" computers (computers lacking specific assurance of the correct implementation of security properties) for making security decisions. For example, Wang himself (column 11, lines 2-5) says "Display may be omitted if desired, in which case the transaction may be viewed, for example, at a display associated with the electronic transaction system itself." This suggests that trustworthy display of the information is not critical to the security of Wang's system.

If Wang had characterized the display of this information as critical, then it would be obvious for one of ordinary skill in the art to provide a trustworthy display. But Wang described it as optional, and so it is not obvious to make the display trusted.

In the design of security devices, it has been well known for over 30 years (almost the entire history of secure computing) that it is appropriate to *minimize* the number and size of hardware and software components that need to be trusted. In <http://csrc.nist.gov/publications/history/ande72.pdf>, Anderson said "the reference validation mechanism must be small enough to be tested (exhaustively if necessary)." In http://www.acsac.org/secshelf/papers/protection_information.pdf, Saltzer and Schroeder said "...examples of design principles that apply particularly to protection mechanisms: a) Economy of mechanism: Keep the design as simple and small as possible...."

Intuitively, it may be felt that one would prefer to trust as much of the computer as possible. However, to claim that a particular component is trustworthy invokes a number of onerous obligations on the designers. It is much better to be able to show that a system only relies for its security on the correctness of a single, small, simple component,

than to require that many large, complex items must all work correctly for the system to be secure.

Designers of security systems therefore do not simply read about a trusted display and “obviously” think “I could add a trusted display on my system” or “I could make the display on my system trusted.” They would be much more interested in situations where they could remove the requirement for a particular aspect of their system to be trusted.

Also, designers do not look at the set of functions that their systems perform and find it “obvious” to adapt the system so that a particular one might be trustworthy.

The only reason for determining that a particular component needs to be trusted is that the system could be insecure if that component is absent or fails to perform correctly. Taking Wang’s PEAD and subjecting it to a new environment with a different set of threats that makes the display critical is not an obvious step, even if that threat has been addressed by another system in the literature.

(f2) Veil does not teach displaying all transaction details

Veil has not explicitly disclosed displaying *all* relevant transaction information. For example, if Applicant were transferring money to a particular payee, Applicant would not want to confirm only the amount, but also the identity of the payee. In the same way that malicious software might alter the amount being transferred, it could also alter the destination for the funds.

Just as the extension from “transaction” to “document” was not obvious given Wang’s disclosure, it remains not obvious in light of Veil’s additional disclosure.

In summary, Applicant has shown that neither does Wang disclose the display of a document (he discloses the optional display of a transaction), nor does he disclose the

trusted display of a document, nor is it obvious to combine the disclosure of the trusted transaction display by Veil with Wang's disclosure. Claim 1 cannot be rejected on this basis.

The amendment to the claim 1 includes the phrase "visually setting forth obligations to which the user is to be contractually bound upon assent thereto by the user" and operation of an input that indicates "assent to the obligations set forth in the document displayed on the trusted display such that document cannot be repudiated." New claim 25 includes the phrase "a document to be viewed and signed so that the document cannot be repudiated", as well as the limitations of "and a digital private key protection device's private key wherein digital data signed by said digital private key protection device after operation of said user operable input is further signed by said private key of said digital private key protection device" (found in claim 6).

For the foregoing reasons and amendments, Applicant believes that the subject matter of amended independent claims 1 and 25 is not rendered obvious by Wang in view of Veil. Reconsideration of the rejection of claim 1 is respectfully requested. Claims 1-12 and 14-24 depend from and add further limitations to amended independent claim 1 and are believed to be patentable for the reasons discussed hereinabove in connection with amended independent claim 1. Reconsideration of the rejections of claims 1-12 and 14-24 is respectfully requested.

In any case, Applicant wishes to address the rejections set forth with respect to some of the other dependent claims.

Response to Examiner's Paragraph 5.2 Claim 4

The Examiner asserts that Wang discloses an audit means in, for example, column 7 lines 1-17, column 12 lines 35-50, and column 4, lines 40-55.

In the Applicant's specification (page 21), Applicant notes that a preferable property of an audit means is the inability to alter or clear the log, so that (a) it is possible for

an authority to review uses of the DPKPD to look for inappropriate use, and also (b) to provide evidence to an adjudicator that a certain event took place, even though the user, or even all participants, may wish to deny that it did. In this way, the DPKPD is said to add to the non-repudiation features of the claimed device.

Wang's column 7, lines 1-17 discloses that user identification and timestamp data can be included (perhaps in an encrypted form) in information that it transmits to a transaction system. This is routine in any digital signature system. This, however, is not an audit means, because it does not provide a centralized storage of the transaction details, and there is certainly no indication of it being protected against alteration or erasure. If the transaction system happened to maintain an audit log (which may be normal), then it would be possible to provide evidence that the user performed a transaction, even if the user denied it. This is a simple form of non-repudiation that can be provided by a digital signature alone. However, it would be impossible for the user to provide evidence of having performed a transaction if the transaction system wished to deny it, because the transaction system may not have received or stored the information. The transaction system might even have altered or erased that information from its own log, if such an action would be to its owner's benefit.

Wang's column 12, lines 35-50 shows how the identity and timestamp information can be used to detect multiple instances of the same transaction. Again, it does not have any way to provide non repudiation.

Wang's column 4, lines 40-55 also refers to the fact that user identification data is incorporated in the PEAD's output. Again, while it would be *necessary* for this information to be included in an audit log, the mere presence of this information in certain outputs is *not sufficient* to suggest that the PEAD has an audit log.

Accordingly, claim 4 is believed to be in condition for allowance.

Response to Examiner's Paragraph 5.2 claim 5

The Examiner's rejection of claim 5 is on the same basis as his rejection of claim 4. The response above applies equally to the case of claim 5.

Accordingly, claim 5 is believed to be in condition for allowance.

Response to Examiner's Paragraphs 6 and 6.1 claim 2

The Examiner asserts that the concepts of creation and validation of digital signatures and encryption and decryption using (combinations of) private, public and secret keys are disclosed by Wang, Veil and Schneier.

Applicant agrees that in a general sense, these concepts are well known. However, the following explanation may help to place claim 2 in a context in which its novelty and non-obviousness may be more easily understood.

Usually, when one applies a signature to a document (whether electronic or paper), it is because the reader of the document expects to see the signature – perhaps they will only perform some action or form some view if the signature is present. Sometimes, it is a computer system (such as a transaction system) that will check the signature automatically. It may be, for example, that a transfer of funds will occur only if the request is validly signed. In that case, once the transaction system determines that the signature is valid, it can commence processing the transaction.

However, in other circumstances, the ultimate recipient of the signed message is not a computer system, but a person. For example, a military order may be sent from one commander to a subordinate officer. It is the subordinate officer who needs to know whether the signature is valid or not. When his computer receives the signed order, it will perform the necessary calculations to determine whether the signature is valid. The calculations are typically too complex for a person to perform with any practicality, so it must be a computer that does those calculations. But then, the computer needs to display the result to the person.

Now if it is a commodity computer, with the various vulnerabilities to endpoint attacks, any information that the computer displays to the user must be regarded with some suspicion. For example, if the computer shows the subordinate officer that the commander has authorized use of deadly force against an enemy, that officer will want to be assured that this was really the commander's intent, and that it is not some malicious software displaying such a result without the commander ever having sent such a message.

Applicant's claim 2 describes a DPKPD which, *as well as* having the capability of *applying* the signature without vulnerability to endpoint attacks (e.g., the commander may use this capability), can also *validate* such a signature for a recipient, and display to that recipient whether the message was validly signed or not.

Wang and Veil have described systems that help assure an individual that their private key will only be applied to create a signature when that individual approves such an act. Wang explains that his signed transaction will be sent to a transaction system – presumably one which will automatically validate the signature and not need to display the result to a person.

Veil is a little less specific about the transaction system. In fact, he also proposed that after the approval (signed with the user's signature) is sent to the transaction system, the transaction system might send back a signed approval of the approved transaction – presumably a “receipt” to indicate that the transaction was accepted. Veil's coprocessor verifies (See Veil, column 10 lines 16-20) the signature on that receipt. However, the result of this verification is passed to the computer. There is no contemplation of displaying the result on a trusted display. This is reasonable for Veil since, in most systems, the provision of a receipt has little effect on the behavior of the recipient. For example, if Applicant authorizes a cash withdrawal of \$50.00 from an account at an ATM, it isn't really important

(most of the time) to get a receipt – Applicant just takes the money and leaves. Sometimes machines run out of paper to print receipts – and this doesn't stop people using them.

Applicant further notes that Wang and Veil (and Fischer) propose the use of public key certificates as a way to provide assurance in the relationship between a public key and its owner, and other aspects. This technique has been well known since 1988. See:

W. Diffie and M. E. Hellman. New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. IT-22, Nov. 1976, pp. 644-654.

R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21 (2), pp. 120-126. 1978. Previously released as an MIT "Technical Memo" in April 1977. Initial publication of the *RSA* scheme.

Gordon, J.A. How to forge RSA key certificates, Electronics Letters, Cybernation Ltd., St. Albans, UK, v 21, n 9, 25 April 1985, pp. 377-9.

CCITT Recommendation X.509 (1988), "The Directory - Authentication Framework".

Public key certificates contain signatures. Before one can rely on the contents of such a certificate, it is important to validate the certificate. (This will enable the user to detect, inter alia, malicious alteration of the certificate after it was issued.) This validation requires many steps, one of which is verifying the signature on the certificate. Although Wang does not refer explicitly to the verification of signatures, he does refer (See Wang column 7, lines 43-52) to decrypting encrypted material using a public key. Since the public key is public, it is feasible for anyone to decrypt the encrypted data with that public key, therefore gaining confidence that the proposed transaction information was encrypted (or more appropriately, signed) using the corresponding private key. Note that this only provides the PEAD with an indication of where the transaction request has come from and that it has not been altered in transit. Of particular note is that there is no contemplation of showing the

source (owner of the public key) to the user. Further, there is no discussion of the PEAD or any other trustworthy system being used to verify the signature that the PEAD generates.

Veil (column 4, line 56 to column 6, line 2 and column 12, line 30 to column 13, line 41) mentions the verification of certificates and certificate chains that may be used to transport public keys.

Fisher (column 8, lines 37-42) refers to verifying signatures and checking certificates. In this case, Fisher is describing how any entity wishing to use the output from the notary device would do so. While Fisher has a trusted device to create the signature(s), and explains how the signatures are verified, he does not propose to verify the signatures on a trusted device. This means that anyone wishing to see the result of the verification is vulnerable to an endpoint attack. Applicant's claim 2 proposes a trustworthy device, with a trustworthy display, on which a user can rely.

Clearly, although these references from the prior art use some of the same words for verifying signatures, it is for a completely different function (Wang, Veil) or different scope (outside the trusted device) from that described in Applicant's claim 2. Note that the description in page 25, paragraphs 2-4 of Applicant's specification provide fair basis for this claim. Furthermore, page 25, paragraph 5 to page 26, paragraph 1 describes that the PKPD can calculate both (a) the validity of the chain of certificates (the same function that Wang describes) and (b) the validity of the message as separate concepts.

However, claim 2 describes a *trusted display* which shows the validity of a signature that was created elsewhere. As described on page 25, the result of signature validation is subject to an endpoint attack. For example, if Applicant receives a message, malicious software on Applicant's computer may assert that the message was signed by a suitable authority – even if the signature was not valid, or the signature was valid but made by a different person, or even if there was no signature at all. Or, if an appropriately signed

message is received, Applicant's computer may say that it was not signed, or signed by the wrong person.

Wang discloses the generation of signatures by the PEAD (column 7, lines 1-7), and implies the checking of those signatures by a transaction system (column 7 lines 15-17). Wang also discloses that the PEAD may decrypt encrypted transaction requests (column 7 lines 43-52). Wang also discloses displaying some information about a transaction (column 4 lines 41-44). However, Wang does not disclose that the PEAD would display the results of a signature validation. Wang leaves it to the transaction system (external to his invention) to validate the signature created by the PEAD.

Veil (column 4, lines 46-55) describes that the security processor can generate authorization information (column 10, line 7-8), and also validate (verify) a signature (column 10, lines 17-19), but the result is only passed to the computer, and in particular is not displayed to the user. Although Veil's system has a trusted display, it is only used to inform the user that he may safely enter his PIN (column 9, line 67), or to display some information about the transaction (column 7, lines 58-62).

While Schneier does describe the methods for calculating the validity of a signature, and many applications for such results, including the protection of keys in certificates, he does not disclose the display of such a result in a trusted display.

Accordingly, claim 2 is believed to be in condition for allowance.

Response to Examiner's Paragraphs 7 and 7.1 claims 11 and 12

Claim 11 describes a DPKPD that receives, decrypts, and displays (sensitive) information, but will not release that decrypted information to an external system unless the user specifically authorizes that action.

Applicant agrees that Wang teaches decrypting sensitive data in the PEAD.

Applicant agrees that Dillaway teaches requiring a specific input from a user before carrying out certain security critical operations. Dillaway nominates (column 2, lines 17-18) encryption, decryption, authentication and verification as “principal cryptographic primitives.” He then notes (column 2, lines 55-56) “there are potential hazards of using cryptographic functions....” Further he notes (column 3, lines 20-25) that smart cards can perform encryption, decryption and verification, which he calls “critical cryptography operations.” He aims to ensure that (column 4 lines 1-3) “the security and authentication-related functions of a Smart Card are utilized only with the explicit authorization of the Smart Card owner.”

The Examiner asserts that transmitting decrypting (*sic*—decrypted) information outside of the card is (recognized as) a security critical operation to one skilled in the art.

The Examiner further asserts that given the combination of (a) Wang decrypting material on a PEAD, (b) Dillaway requiring operation of a specific input before performing security critical operations, and (c) the release of sensitive material outside a device is a security critical operation, that the subject of claim 11 is obvious.

Applicant disagrees for a number of reasons.

1. The determination of whether something is security critical depends very much on the specific requirements. If the requirement is to prevent decrypted material from being made available outside the card, then it is quite easy to choose a countermeasure such as (a) don't give the smart card the keys necessary to decrypt the material, or (b) don't allow the smart card to perform the decryption operation, or (c) don't connect the smart card to an external system.

2. The only standard situation in which a security device will decrypt an item, but then prevent its transmission outside a system is when a new key is being loaded

into a device. This is not at all analogous to the case of receiving a sensitive message which should be shown to a user, but not transferred to the user's computer.

3. Dillaway's assertion that human input should be used prior to execution of a certain set of nominated security critical operations does not make it obvious to one skilled in the art that the technique is necessarily extensible to any security critical operation. In fact, without a trusted display (which Dillaway does not contemplate), the human input is not very useful. For example, he considers the problem of malicious software piggybacking an extra operation. It is quite possible that when the user wants the smart card to sign message A, and therefore presses the button, that the software in the user's computer has actually asked the smart card to sign message B.

This appears to demonstrate that to Dillaway (and Wang) (presumably people skilled in the art), it was not obvious to combine a trusted display and the human input prior to performing what (with the benefit of hindsight) is a security critical operation.

Indeed, the transformation of a single security critical operation (decryption) into three separate ones (decryption, display, and release) is a particularly inventive aspect of the present invention. Those skilled in the art have traditionally considered the decryption of an encrypted message to be the quintessential security critical operation.

Typically, when considering whether to send a message or document to a person, Applicant considers whether that person is authorized to see the message or document. Most security coprocessors, including Dillaway's and the IBM 4758 for example, once having been instructed and authorized to perform a decryption, will consider the decrypted plaintext material to be releasable to the computer.

The inventive aspect here is to recognize that while the human user ought, by virtue of their identity as established by the corresponding private key, to be able to view the decrypted material; such material need not necessarily be suitable for release to potentially

untrustworthy computer systems. So a sender may decide that, while it is permissible for a message to be viewed by a recipient, it is not appropriate for the recipient's computer to have access to that message (in decrypted form). Thus (according to claim 12) the DPKPD would not release the data to the communications port. This would prevent, for example, the information from being leaked or forwarded by any malicious software that might be on the user's computer.

In another circumstance, the choice may be given to the recipient to determine whether such information ought to be released to the untrustworthy computer system for further processing. In accordance with claim 11, this data will only be released external of the DPKPD if the user specifically authorizes that by operating the relevant button.

The invention thus represents a major advance over existing systems, and provides a high assurance guarantee of the security of the message.

More importantly, it is settled law that "[w]hen a party claims that a combination of references renders... [an] invention obvious, the prior art must provide a suggestion or motivation to combine the references.... Absent this suggestion or motivation, the mere existence of the individual elements at the time of invention does not render a patented combination of these elements obvious as a matter of law." Remcor Products Co. v. Scotsman Group Inc., 32 USPQ2d 1273, 1278 (N.D. Ill. 1994). The Court addressed the use of hindsight reconstruction as a basis for obviousness rejections in In re Fritch, 972 F.2d 1260, 1266, 23 USPQ2d 1780, 1784 (Fed. Cir. 1992) wherein the Court stated "[i]t is impermissible to use the claimed invention as an instructional manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious. This court has previously stated that '[o]ne cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention.'" Moreover, in Texas Instruments Inc. v. U.S. Intern. Trade Com'n., 988 F.2d 1165, 1178, 26 USPQ2d 1018,

1029 (Fed. Cir. 1993), the Court stated the prior art “references in combination do not suggest the invention as a whole claimed in the... patent. Absent such suggestion to combine the references, respondents can do no more than piece the invention together using the patented invention as a template. Such hindsight reconstruction is impermissible.”

In any case, the release of decrypted material to the computer as a separate security critical operation from the transfer of such information to the trusted display is in fact novel and inventive, and solves a major previously-unsolved problem faced by many people and organizations while protecting against end-point attacks that would otherwise have unacceptable consequences.

Accordingly, claims 11 and 12 are believed to be in condition for allowance.

Response to Examiner’s Paragraph 8 claim 6

The Examiner asserts that it would be obvious to one of ordinary skill in the art that combining the implementation of multiple signatures (disclosed by Fischer) and the trusted display of transactions (disclosed by Wang and Veil) “provides further security and trust such that both the device producing the signature and the entity can be trusted and validated as the data is signed twice.”

Unfortunately, the mere presence of two signatures does not, in general, increase the level of trust that a recipient can have about the information being signed, or the circumstances in which it was signed. To see why this is the case, it is important to understand the concept that distinguishes the operation of Wang, Veil or Fischer devices from a DPKPD: the semantics of the signatures.

What can the recipient of a message believe if they see a message that has an originator’s user signature? The recipient can be confident that, at some time, the message was signed with the originator’s private key. The recipient may (either naively or through

sound judgment) choose to believe that the originator deliberately decided to approve and sign that particular message, but the signature does not provide evidence for this.

The Wang PEAD or Veil smart card device help give the originator some control over how their private key may be used to make such signatures. Thus, using one of these systems may provide extra value to the originator. However, there is nothing in the signature that convinces the recipient that the originator used such a device.

In particular, if the originator took their smart card out of a Veil-type system, and placed it in a “regular” system, then that regular system may sign many messages without the originator being aware of it. The recipient of a user-signed message has no way to distinguish whether the message was constructed in a Wang/Veil-type system (with the protection that that provides), or not.

Now, what can the recipient of a message believe if he sees a message that has a device signature? Whether the device is a DPKPD or a Fischer time-stamper, the recipient can be confident that this message was signed by that particular device. If the device is trusted to provide any security properties, such as a reliable clock and timestamps, then the recipient can trust the representation of those functions (e.g., a time indication) within the signature. The recipient can be assured that the time value supplied inside the signature was actually the one provided by the time-stamper, and not one provided by another (potentially malicious) device.

In the case of the third embodiment of Fischer’s time-stamper, it will provide two signatures: a user signature and a device signature. Fischer suggests that the user signature could be either the inner one or the outer one. If the user signature is the outer one, then a recipient can be convinced that the user’s key was applied after the timestamp. The recipient can trust the timestamp, but cannot be confident about whether the user’s signature was created in the timestamp device or elsewhere.

For example, consider a case in which the timestamp device is trusted to apply a user signature immediately after stamping the time. When the message comes out of the time-stamper, it will have both signatures. However, it would be possible for one user's outer signature to have been removed from the message that came out from the time-stamper, and another user's signature applied instead. The recipient will have no way to tell whether this has happened, or whether the outer signature was created by the device.

If, however, the device's signature is constructed by the timestamp *after* the user signature, and the device is trusted to *only* create a device signature after having made a user signature, then a recipient can be convinced that the user's signature was constructed by that device.

It is important to note that while Fischer mentions that a variety of signing (and time-stamping) combinations are possible (column 8, line 26), he does not teach the benefits of the latter, or the reasons they are desirable. He says (column 8, line 26) that it is preferred to have the device signature last, but does not explain why – merely that one such approach (column 8, line 37) “would be compatible with conventional notarization techniques.”

In particular, Fischer notes (column 7, lines 5-7) that a recipient (“verifier”) “can determine that the signing key is associated with the particular user and also that the supplied time stamp is trustworthy.” It is true (regardless of the signature order) that the user's signature does guarantee that the message was signed with a key associated with that user. Importantly, it does not indicate *how* that signature was made, nor that it was made in accordance with the user's deliberate intentions. Fischer had the “opportunity” to disclose the effect of the order of the signatures. However he was unaware of many issues associated with endpoint attacks, because it was not obvious to him as one with at least ordinary skill in the art to consider the time-stamping double-signature in combination with the user-approval

of signatures, he did not see the difference in the semantic effects of the different order, let alone feel the need to investigate their comparative benefits.

One with ordinary skill in the art may well apply the concepts disclosed by Wang (and Veil) and the concept disclosed by Fischer in sequence (“series”). That is, the Wang PEAD could be used to create a signed transaction authorization, and then the Fischer times-stamper could apply a trustworthy timestamp to that authorization. The recipient, on validating both the signatures, will come to the conclusion that the authorization was indeed created prior to the time indicated in the outermost (i.e. second) signature – the one created by the time-stamper. However, the additional signature does nothing to convince the recipient that the originator deliberately chose to apply his personal signature to that particular message. In particular, if the originator chooses later to deny having sent the message, he can claim that it was signed with his private key by a computer email program, and that he didn’t use the PEAD. Or, he could say that he thought he was using his PEAD to sign a different document. The *only* effect of the second signature is to assure that the inner message (or “envelope”) was created at the time indicated in the timestamp.

The DPKPD device signature has different, stronger, properties. The DPKPD’s device signature provides not only the semantic indication that the inner message was created at the appropriate time, but also that the signature *was created using a DPKPD, using the trusted display regime that DPKPDs apply*. It is impossible for a DPKPD signature to be applied to a message or document *unless that document has been viewed and approved by the user on the DPKPD*. This is in sharp contrast to Fischer, whose abstract mentions “The user does not need to be involved in any additional decision making as to whether time-stamping [signing] is necessary.”

There is no aspect of a PEAD (Wang) or Veil signature that can convey to the recipient any information about how that signature was created. The recipient may (either

naively or with sound basis) choose to believe that the originator follows certain procedures – such as never using their private key in any device except a PEAD – and that their computer is not vulnerable to malicious software that could perform an endpoint attack. But the signature itself does not guarantee this.

In contrast, if the recipient receives a message which contains a DPKPD (outer) signature, that recipient will be assured that the inner signature could *only* have been created on a DPKPD. The recipient will have additional confidence, then, that the originator did actually review the material, and did deliberately choose to approve and sign the material. Furthermore, the recipient will be able to convince a third party adjudicator of this, even if the originator attempts to deny having approved the message. Again, this is not the case with Wang's PEAD or Veil's smart card system.

It may have been possible for one of ordinary skill in the art to construct a device that performed both the function of a Wang PEAD and a Fischer time-stamper. While this may appear to provide the same assurances to a recipient as that of the DPKPD, there is still an important difference. The key is what the devices are *trusted* to do. The Wang PEAD is *trusted* not to sign a transaction authorization unless the user approves it by pressing the button. The Fischer time-stamper is *trusted* to apply timestamps with the correct time. The Fischer time-stamper may also be *trusted* to apply user signatures.

For a combination of the PEAD and time-stamper devices to provide similar assurances to that of a DPKPD, it would be critical for there to be trust that the timestamp (i.e. device signature) is *only* applied directly after the user signature has been applied. That is, it must be impossible for the device signature (timestamp) to be applied to something that has not just been user-signed by the device.

This is very much contrary to intuition, and certainly not obvious to one of ordinary skill in the art. In general, when a device can perform two functions A and B, it is

better to make the device flexible, so that it can be used to perform either function A, or function B, or a combination AB or BA. For example, knowing that a computer can run a word processor (A) and also that a computer can also run a spreadsheet (B), a designer would be unlikely to want the computer to be able to run a word processor and then a spreadsheet (AB), but never a spreadsheet in isolation (B), and never a spreadsheet and then a word processor (BA). Yet that is a critical aspect of the composition of the Wang/Veil and Fischer concepts that would be required for it to provide the properties of the DPKPD as claimed by the present applicant.

Accordingly, claim 6 is believed to be in condition for allowance.

Response to Examiner's Paragraph 8 claims 7 and 8

Verification of a (single) digital signature is well known. Fischer gives a broad outline of how the process would apply to his double-signature (or double certificate) system in column 11, lines 38-55. Fischer notes (column 11, line 67 – column 12, line 1) that the notary device is *trusted*. However, as he is only aware of impersonation attacks (solved by digital signatures) and not endpoint attacks, he does not suggest that the verification needs to occur in a trusted way. In fact, he goes so far as to say (column 11, line 20) “The verification operation requires no special security measures be undertaken.”

While it will not “damage” the timestamp itself to process it on an insecure or untrustworthy system, it will certainly not be possible to rely on the result obtained there from. Even if the message was legitimately signed by Fred at 12:34 on 1/2/06, the untrusted, insecure computer which is supposed to be verifying the timestamp may have malicious code that reports to the user that it was signed by George at 11:02 on 3/4/05. For such a system to be useful in high-value (security critical) operations, it is essential for the endpoint on which the timestamp is verified to be trustworthy.

As in Applicant's response relating to claim 2 (Examiner's paragraphs 6 and 6.1), neither Wang nor Veil use trusted devices to verify the signatures created by their trusted PEAD or smart card system.

It is certainly not obvious for one of ordinary skill in the art to (a) take this teaching of Fischer ('security not required for verification'), (b) add the verification function to a secure platform of Wang/Veil, and then further (c) use the trusted display of Wang and Veil to display the result of such a verification, especially since (d) the beneficial semantics of the device signature have not been taught.

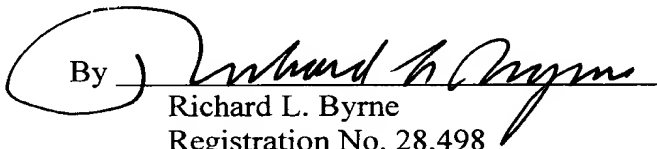
Accordingly, claims 7 and 8 are believed to be in condition for allowance.

Conclusion

For all the foregoing reasons, Applicant believes that claims 1-12 and 14-24, as amended, and new claim 25, are patentable over the cited prior art and in condition for allowance. Reconsideration of the rejections and allowance of all of pending claims 1-12 and 14-25 is respectfully requested.

Respectfully submitted,

THE WEBB LAW FIRM

By 
Richard L. Byrne
Registration No. 28,498
Attorney for Applicant
700 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219
Telephone: 412-471-8815
Facsimile: 412-471-4094
E-mail: webblaw@webblaw.com